MAY 2024

TRU Technical Partners
IT SUPPORT & CYBERSECURITY

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks

How to make the pain of passwords go away

Passwords. They're the keys to our digital kingdoms, but also the biggest pain in our necks. They've been around since the dawn of the internet, and guess what? Even with replacements being introduced, they're not going away anytime soon.

I'm sure you've felt the pain of managing a billion passwords for all your accounts. It's exhausting and risky. Perhaps it's time you considered using a password manager.

The real beauty of password managers is you only have to remember one password – the master password to log in to your manager. **Then, it does everything else for you.**

- It creates long random passwords
- It remembers them and stores them safely
- And it will even fill them into the login page for you

That means no more racking your brain trying to remember if your password is "P@ssw0rd123" or "Pa55w0rd123" (both are really bad and dangerously weak passwords by the way). With a password manager, all the work is done for you.

We won't sugar coat it – password managers aren't invincible. Like all superheroes, they have their weaknesses. Cyber criminals can sometimes trick password managers into auto filling login details on fake websites.

But there are ways to outsmart criminals. First, disable the automatic autofill feature. Yes, it's convenient, but better safe than sorry, right? Only trigger autofill when you're 100% sure the website is legit.

And when choosing a password manager, go for one with strong encryption and multi-factor authentication (MFA) where you generate a code on another device to prove it's you. These extra layers of security can make a big difference in making your accounts impenetrable.

Enterprise password managers offer useful features like setting password policies and analyzing your teams' passwords for vulnerabilities. Plus, they often come with behavior analysis tools powered by machine learning tech. Highly recommended.

But here's the thing – no matter how advanced your password manager is, it's only as good as the person using it. So, do yourself a favor: Train your team to stay vigilant against scams, and always keep your password manager up to date.

We can recommend the right password manager for your business and help you and your team use it in the right way. Get in touch.

DID YOU KNOW...

you could soon type with your eyes?

Sounds crazy, but Microsoft is developing an Eye-Gaze technology that will help people type and interact with applications using just their eyes.

It uses so-called 'dwell-free' typing, meaning you'd just need to look at keys on a screen and the technology would – supposedly – understand the actions you want to take. The tech also uses AI to gather information that makes predicting behavior patterns more accurate.

Do you think that's cool... or scary?!

You'd be lost without it, so don't forget email security

Let's talk about something super important: Email security. Yep, we know it might not sound like the most thrilling topic, but it's a big deal. Businesses like yours face more cyber threats than ever.

We've seen our fair share of cyber attacks, and let us tell you, many of them start with a simple email (official figures say it's a massive 90%!). Yep, that innocent-looking message in your inbox could be the gateway for cyber criminals to wreak havoc on your business.

So, why is keeping your business email secure so important? Well, for starters, it's your first line of defense against cyber attacks. Think of it like locking the front door of your house to keep out intruders. If your email is secure, you're making it a whole lot harder for cyber criminals to sneak in and steal your sensitive data.

But implementing proper email security measures safeguards your valuable data from getting lost or falling into the wrong hands. It's not just cyber criminals you're at risk from; an employee could accidentally leave a laptop on a train or in a coffee shop. That could mean all your important business communications and documents were suddenly open for someone else to read. It would be a nightmare, right?

You might be thinking, "But I'm just a small business. Why would I be a target?" Ah, but here's the thing – cyber criminals don't discriminate based on business size. In fact, small and medium-sized businesses are often seen as easier targets. That's because they may not have the same level of security measures in place as larger corporations. So, don't think you're off the hook just because you're not a Fortune 500 company.

Now that we've established why email security is crucial, let's talk about how you can ramp up your defenses. First off, use strong, unique passwords for your email accounts. None of that "p@ssW0rd123" nonsense, please. Better still, use a password manager to create and store uncrackable passwords.

Consider implementing two-factor authentication for an extra layer of security (where you generate a login code on another device to prove it's you). And don't forget to keep your software and security patches up to date – those updates often contain important fixes for vulnerabilities that cyber criminals love to exploit.

Lastly, educate your employees about the importance of email security. They could be your strongest defense or your weakest link when it comes to keeping your business safe from cyber threats. Teach them how to spot phishing emails (emails pretending to be from someone you trust) and what to do if they suspect something isn't right.

Remember, a little prevention now can save you a huge headache (and money) later. If we can help with that, get in touch.

Q: Will a free VPN (Virtual Private Network) provide enough security for my employees' work phones?

A: No. The chances of a free VPN logging and selling your data or infesting your device with malware are a lot higher than if you used even the cheapest paid VPN on the market.

Q: I hate sudden reboots for updates on Windows 11, is there a way to avoid them?

A: Yes! Open "settings" and click on "Windows update" and then "advanced options", you can then set your "Active hours". Updates can be scheduled, where possible, outside of these hours.

Q: I hate my password manager, is it easy to change?

A: You can export your data, but it's important to use a secure computer to do it. You should also be careful not to back up the unencrypted file. We can help you – get in touch.

Business gadget of the month

MELIFO monitor light bar

Your home office set up may take a little adjustment to get just right. This monitor light bar will help create exactly the right lighting for your desk without creating glare on your screen or illuminating the whole room.

It reduces eye strain, it's cheap, and it's easy to set up. Oh, and it looks really cool too!

$39 from Amazon.

This is how you can get in touch with us:

CALL: 408-559-2800 | **EMAIL** info@trutechnical.com
WEBSITE: www.trutechnical.com

TRU Technical Partners
IT SUPPORT & CYBERSECURITY